AO 93C (08/18) Warrant by Telephone or Other Reliable Electronic Means

☑ Original ☐

CLERK'S OFFICE
A TRUE COPY
Mar 22, 2023
s/ JDH
Deputy Clerk, U.S. District Court
Eastern District of Wisconsin

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
Information associated with the following Gmail accounts: freedomtaxxes@gmail.com, maxxedtaxservices@gmail.com, and maxxedfinancial@gmail.com which are stored at premises owned, maintained, controlled, or operated by Google, LLC, a company headquartered in Mountain View, California.

Case No. 23-M-347 (SCD)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Northern District of California *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 4-4-23 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Stephen C. Dries.
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for _____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 3-22-23. 10:35 am

Stephen C. Dries
Judge's signature

City and state: Milwaukee, WI

Hon. Stephen C. Dries, U.S. Magistrate Judge
Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the following Gmail accounts:

a. Gmail Account: **freedomtaxxes@gmail.com (Target Account 1)**

b. Gmail Account: **maxxedtaxservices@gmail.com (Target Account 2)**

c. Gmail Account: **maxxedfinancial@gmail.com (Target Account 3)**

which are stored at premises owned, maintained, controlled, or operated by Google, LLC, a company headquartered in Mountain View, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google, LLC (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to the Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on January 20, 2023 (number 29781545), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A **for the time period of December 24, 2020, through the date of this warrant for all target accounts:**

(a) All records or other information regarding the identification of the accounts, commonly known as subscriber or registration information, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses, methods of connecting, log files, and means and source of payment (including any credit or bank account number).

(b) The types of services utilized.

(c) The contents of all emails associated with the accounts, including stored or preserved copies of emails sent to and from the accounts, draft emails, the source, and destination addresses associated with each email, the date and time at which

each email was sent, the size and length of each email, and any attachments associated with emails.

(d) The details of electronic devices used to access such services such as serial numbers and other unique device identification numbers.

(e) All other records or other information stored using the accounts, including address books, contact lists, calendar data, pictures and videos, and files.

(f) All records pertaining to communications between the provider and any person(s) regarding the accounts, including contacts with support services and records of actions taken.

The provider is hereby ordered to disclose the above information to the government **14 DAYS** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. 286 (Conspiracy to Defraud the Government), 18 U.S.C. 287 (Filing False Claims), 18 U.S.C. 1343 (Wire Fraud), and 26 U.S.C. 7206(2) (Aid or Assist in Filing False or Fraudulent Returns) involving **JASMINE CALHOUN** including, information pertaining to the following matters:

1. The creation, preparation, and filing of tax returns, including all preparatory steps and communications.
2. Information provided by clients and potential clients concerning potential tax returns and Paycheck Protection Program loans.

3. Records and information pertaining to taxes, refunds, and W-2s.
4. Advertisements and/or solicitation of tax clients.
5. Stimulus checks and Paycheck Protection Program Applications
6. Personal identifiable information of taxpayers, including names, date of birth, social security numbers, and driver's licenses.
7. Mailings to and from 3907 N. 84th St Milwaukee, WI 53222 including in names other than **JASMINE CALHOUN**.
8. Proceeds and/or payments pertaining to the preparation of tax returns or Paycheck Protection Program Applications.
9. Financial records, including account information, bank statements, checks, money orders, cash, ATMs, withdrawals, deposits, transfers (including wire, ACH transfers);
10. All evidence of who created, used, owned or controlled the Target Accounts, including, records that help reveal the identity and whereabouts of such person(s).
11. Evidence indicating how and when the Target Accounts were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the Target Account owner.
12. Evidence indicating the Target Account(s) owner's state of mind as it relates to the crimes under investigation.
13. The identity of the person(s) who communicated with the Target Accounts about matters relating to the above-mentioned violations, including records that help reveal their whereabouts.

UNITED STATES DISTRICT COURT

for the

Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Information associated with the following Gmail accounts: freedomtaxxes@gmail.com, maxxedtaxservices@gmail.com, and maxxedfinancial@gmail.com which are stored at premises owned, maintained, controlled, or operated by Google, LLC, a company headquartered in Mountain View, California.

Case No. 23-M-347 (SCD)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC §§ 286, 287, & 1343; 26 USC § 7206(2)	Conspiracy to defraud the government; filing false claims; wire fraud; and aid or assist in filing false or fraudulent returns.

The application is based on these facts:

See attached Affidavit.

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Jeremy J. Grobart
Digitally signed by Jeremy J. Grobart
Date: 2023.03.21 13:56:35 -05'00'

Applicant's signature

Jeremy Grobart, SA

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 03/22/2023

Stephen C. Dries

Judge's signature

City and state: Milwaukee, WI

Hon. Stephen C. Dries, U.S. Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Jeremy J. Grobart, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that are stored at premises owned, maintained, controlled, or operated by Google, LLC ("Google"), an email and electronic services provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the account.

2. **Your Affiant.** I am a Special Agent with the Criminal Investigation Division of the Internal Revenue Service (IRS-CI), United States Department of the Treasury, and have been since July of 2021. I am a Certified Fraud Examiner through the Association of Certified Fraud Examiners and have a bachelor's degree in Criminal Justice from University of Cincinnati, along with an MBA with a concentration in Data Analytics from Loyola University Chicago. I have completed the Criminal Investigator Training Program and the Special Agent Investigative Techniques Program at the Federal Law Enforcement Training Center in Glynco, Georgia where I received extensive training on financial investigative techniques. My training included lessons in cybercrime investigations, virtual currency, financial investigative techniques, accounting, tax, money laundering, criminal investigation techniques, criminal law, and search warrants.

3. During this investigation, I have worked closely with IRS-CI Special Agent Zachary Stegenga, who has been employed by IRS-CI since 2008. Since 2008, Special Agent Stegenga has conducted numerous investigations involving violations of the Internal Revenue Code (Title 26, United States Code), the Money Laundering Control Act (Title 18, United States Code), the Bank Secrecy Act (Title 31, United States Code), and other related offenses. Special Agent Stegenga has been the affiant on numerous search warrants, including having participated in the execution of numerous search warrants. I have based my conclusions in part on the training and expertise of Special Agent Stegenga.

4. I make this affidavit in support of an application for a search warrant for information associated with:

a. Gmail Account: **freedomtaxxes@gmail.com (Target Account 1)**

b. Gmail Account: **maxxedtaxservices@gmail.com (Target Account 2)**

c. Gmail Account: **maxxedfinancial@gmail.com (Target Account 3)**

Information pertaining to these accounts is stored at premises owned, maintained, controlled, or operated by Google, LLC, an email and electronic services provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043 (the "Target Provider"), further described herein and in Attachment A respectively (attached hereto and incorporated herein).

5. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require the Google to disclose to the government records and other information in its possession, including the contents of communications, pertaining to the subscriber and customer associated with Target Account 1**,** Target Account 2, and Target Account 3; further described in Section I of Attachment B (attached hereto and incorporated herein). Upon receipt of the information described in Section I

of Attachment B, government-authorized persons will review that information to locate and seize the items described in Section II of Attachment B.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Section 286 (conspiracy to defraud the government), Section 287 (filing false claims), Section 1343 (Wire Fraud), and Title 26, United States Code, Section 7206(2) (aid or assist in filing false or fraudulent returns) (collectively, the "Subject Offenses"), have been committed by **JASMINE CALHOUN (CALHOUN)**. There is also probable cause to search the information described in Attachment A for evidence, fruits, and/or instrumentalities of these crimes, as described in Attachment B.

7. **Subject Offenses**

a. **Title 18, United States Code, Section 286** generally prohibits a person from entering into any agreement, combination, or conspiracy to defraud the United States, or any department or agency thereof, by obtaining or aiding to obtain the payment or allowance of any false, fictitious, or fraudulent claim.

b. **Title 18, United States Code, Section 287** generally prohibits a person from making or presenting, to any department or agency of the United States, any claim upon or against the United States, or any department or agency thereof, knowing such claim to be false, fictitious, or fraudulent.

c. **Title 18, United States Code, Section 1343** generally prohibits a person who has devised or is intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, from transmitting, or causing to be transmitted, by

means of wire, radio, or television communication in interstate or foreign commerce, any writings, for the purpose of executing such scheme or artifice.

d. **Title 26, United States Code, Section 7206(2)** generally prohibits a person from willfully aiding or assisting in, or procuring, counseling, or advising the preparation or presentation under, or in connection with any matter arising under, the internal revenue laws, of a return, affidavit, claim, or other document, which is fraudulent or is false as to any material matter, whether or not such falsity or fraud is with the knowledge or consent of the person authorized or required to present such return, affidavit, claim, or document.

8. **Sources of Information**. The facts in this affidavit come from my personal observations, my training and experience, information obtained from other agents and witnesses, Internal Revenue Service records, public records, and my own investigative efforts. I believe these sources of information to be credible and reliable based on the corroboration of the information and my experience with these matters. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all my knowledge about this matter.

9. **Jurisdiction**. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

10. I am currently investigating **CALHOUN** for operating as an unscrupulous ghost tax return preparer since at least 2018. A ghost preparer is someone who does not sign the tax

returns that they prepare and/or file. The evidence indicates that **CALHOUN** knowingly made and caused others to make false claims to the IRS through the filing of fraudulent U.S. Individual Income Tax Returns (Form 1040s), for the 2017-2021 tax years. The Form 1040s in question contain numerous fraudulent indicators, which will be described in the following paragraphs.

11. On January 23, 2018, the first tax return related to this scheme was filed with the IRS. Based on my knowledge and experience, tax return preparers communicate with their clients days and weeks ahead of when tax returns are submitted to the IRS. Therefore, I believe that communication relating to this scheme would have occurred at least as early as January 1, 2018.

Referral from Southern Area Scheme Development Center (SDC)

12. On April 20, 2022, the Chicago Field Office of IRS-Criminal Investigation received a questionable refund scheme referral from the SDC of the IRS regarding **CALHOUN**. This referral included an analysis of 274 Form 1040s electronically filed with the IRS for the 2017, 2018, 2019, 2020, and 2021 tax years. These 274 Form 1040s were directly associated with **CALHOUN** based on the following return characteristics:

a. 235 of the 274 tax returns were filed using IP address 76.196.89.6. I subpoenaed the provider of the IP Address – AT&T – and confirmed that the account is registered to **JASMINE M. CALHOUN**. The subpoena further confirmed that this IP address has been registered to **CALHOUN** from December 21, 2017, through at least September 22, 2022, and was used at 3907 N. 84th Street Milwaukee, WI 53222, the residence of **CALHOUN**.

b. The remaining 39 of the 274 tax returns were filed using IP address 75.86.10.150. I subpoenaed the provider of the IP Address – Spectrum – and determined that the

account is registered to an individual named Jerald Harris. One of the usernames listed on this IP Address is damondharris83@gmail.com. IRS records show that Damond Harris is the son of Jerald Harris and that Damond Harris is also the father to **CALHOUN**'s son, Fabian Harris. Per the subpoenaed records, 36 of these tax returns came back to this Spectrum IP address that had been registered to Jerald Harris from February 3, 2021, to May 28, 2022, and was used at 3746 W. Walnut Street Milwaukee, WI 53208, which is the residence of both Jerald and Damond Harris.

i. An IP address is a unique identifier associated with a computer or network, which allows users to send and receive data and access the internet.

c. 13 of the 274 returns list the phone number 414-719-3818 – serviced by AT&T. I subpoenaed AT&T for records relating to phone number 414-719-3818 and the records show that the registered user of this phone number is **JASMINE CALHOUN** who has used this phone number from March 5, 2021, to at least September 28, 2022, and listed 3907 N. 84th Street Milwaukee, WI as her address on the account.

d. 45 of the 274 returns list the phone number 262-409-7252 – serviced by T-Mobile. I subpoenaed T-Mobile for records relating to phone number 262-409-7252, and the records show that the phone number is registered to **JASMINE CALHOUN**, who used this phone number from May 7, 2019, through at least September 26, 2022, and listed 3907 N. 84th Street Milwaukee, WI 53222 as her address on the account.

13. Based on my training and experience, the 274 Form 1040 tax returns identified by the SDC, contain indicia of false and fraudulent filings. The following describes these indicators of fraud:

a. 100% of the 274 returns associated with **CALHOUN** claimed refunds. $2,039,484.00 worth of total refunds were claimed on returns associated with **CALHOUN**, and $1,713,205.00 worth of refunds were issued based on these returns. Data collected by the Internal Revenue Service shows tax return refund percentages both nationally and by state. This data was compared to the percentage of tax refunds claimed on tax returns associated with **CALHOUN** and is presented as follows:

PERCENT OF TAX REFUNDS CLAIMED			
	Jasmine Calhoun	Wisconsin	Nation
TY 2021	100%	Data Unavailable	Data Unavailable
TY 2020	100%	72%	73%
TY 2019	100%	70%	71%
TY 2018	100%	68%	68%
TY 2017	100%	69%	70%

b. The American Opportunity Credit (AOC) is a tax credit for individuals who attend a college or an institution of higher learning during the tax year. Certain rules must be met to be eligible for the credit, which reduces a taxpayer's tax liability, or if the taxpayer's liability has been reduced to $0, will increase their refund. The amount of the credit is based on the expenses the taxpayer incurred to attend college that year. The American Opportunity Credit is up to $2,500 of the cost of tuition, certain required fees and course materials that are needed for attendance and paid during the tax year. Also, if the credit for which you qualify

is more than the tax you owe, 40% of that credit (up to $1,000) can be refunded to you. Educational institutions that are eligible to participate in student aid programs issue a Form 1098-T which further supports the AOC.

c. Between tax years 2017-2021, 266 out of 274 tax returns associated with **CALHOUN** had claimed the AOC credit. Of the 266 tax returns that claimed the AOC credit, 263 (or 99%) of the tax returns listed Milwaukee Area Technical College as the attendant institution. There were no Forms 1098-T filed by any institution to support 258 of the 266 AOC claims. This indicated that the AOC was likely fraudulently claimed on the tax returns associated with **CALHOUN**. Data collected by the Internal Revenue Service shows the percent of tax returns that claimed the AOC both nationally and by state. This data was compared to the percent of AOC claimed on tax returns associated with **CALHOUN** and is presented as follows:

PERCENT OF TAX RETURNS WITH AOC			
	Jasmine Calhoun	Wisconsin	Nation
TY 2021	98%	Data Unavailable	Data Unavailable
TY 2020	100%	4%	4%
TY 2019	98%	4%	4%
TY 2018	96%	4%	4%
TY 2017	92%	4%	5%

d. The Earned Income Credit (EIC) is a refundable credit available to eligible individuals with earned income and adjusted gross income below certain limits. The EIC is a prepayment of the tax liability; if the prepayments exceed the tax liability, the taxpayer is due a refund of the excess payments. Of the 274 tax returns associated with **CALHOUN** between tax years 2017- 2021, 249 (or 91%) of them claimed EIC. Data collected by the Internal Revenue Service shows that

the amount of claimed EIC on returns associated with **CALHOUN** is significantly higher than both the rest of Wisconsin and nationally:

PERCENT OF TAX RETURNS WITH EIC			
	Jasmine Calhoun	Wisconsin	Nation
TY 2021	98%	Data Unavailable	Data Unavailable
TY 2020	87%	10%	16%
TY 2019	88%	11%	17%
TY 2018	90%	11%	17%
TY 2017	91%	12%	17%

e. The Additional Child Tax Credit (ACTC) is a refundable credit that an individual may receive if their Child Tax Credit is greater than the total amount owed in income taxes. Of the 274 tax returns associated with **CALHOUN** between tax years 2017-2021, 213 (or 78%) of them claimed the ACTC. Data collected by the Internal Revenue Service shows that the amount of claimed ACTC on returns associated with **CALHOUN** is significantly higher than both the rest of Wisconsin and nationally:

PERCENT OF TAX RETURNS WITH ACTC			
	Jasmine Calhoun	Wisconsin	Nation
TY 2021	77%	Data Unavailable	Data Unavailable
TY 2020	75%	8%	12%
TY 2019	84%	9%	14%
TY 2018	78%	9%	14%
TY 2017	75%	7%	12%

f. Of the 274 returns associated with **CALHOUN** between tax years 2017-2021, 272 (or 99%) of them claimed wages. 87 of the 272 returns claimed wages that contained numerically identical values mostly ending in zero or nine. Most notably, 34 returns contained the wage amount "$18,999." Based on my training and experience as both a Special Agent and Certified Fraud Examiner, numbers

containing repeated identical values in such volume are likely indicators of fraud. In addition to these wages, the most common occupations listed on the tax returns were: Adult Entertainer on 62 tax returns (23% of the total tax returns), Laborer on 40 tax returns (15% of the total tax returns), and Home Health Care Provider on 39 tax returns (14% of the total tax returns). The similarities in employment listed on the 274 tax returns associated with **CALHOUN** create further probability that such tax returns are likely fraudulent.

g. **CALHOUN**'s own Form 1040 tax returns for tax years 2017-2021 all have the same characteristics as the fraudulent returns that have been identified and are associated with **CALHOUN**. For example, on each Form 1040 during tax years 2017-2021, **CALHOUN** listed her own occupation as an Adult Entertainer. **CALHOUN** also claimed the AOC, EIC, and ACTC for herself in tax years 2017-2021. Furthermore, **CALHOUN** listed Milwaukee Area Technical College (MATC) as the institution she attended during each tax year from 2017-2021. However, MATC did not file any corresponding Form 1098-T to support her attendance or the payment of tuition and related expenses during those years. **CALHOUN**'s own reported wages contained similar indicators of fraud that had been found on the other tax returns related to this scheme. This included her reported wages ending in zero or nine for each tax year. Specifically, **CALHOUN** claimed the following wages during tax years 2017-2021: $16,999 (2017), $0 (2018), $18,999 (2019), $18,889 (2020), and $11,000 (2021).

Paycheck Protection Program

14. During a review of IRS databases, I discovered that 27 PPP business loan applications had been submitted by 22 individuals (including **CALHOUN**) whose tax returns were previously identified as being associated with **CALHOUN** during tax years 2017-2021. I noted that the 27 PPP loan applications had very similar characteristics that indicated such applications were likely fraudulent. For example, almost all the businesses in which PPP loans were applied for, claimed to have one employee and annual payroll of $100,000 or near that amount. Furthermore, each application had a monthly payroll of $8,330.33 or close to that amount. The business addresses listed on each PPP loan application matched the individual address on the individual tax returns associated with **CALHOUN**. Furthermore, I also discovered that no Schedule C (a form to report business profits or losses) had been filed with the IRS for these 27 businesses. However, through subpoenaed records from PPP lenders, I saw that these same individuals, had submitted, likely fraudulent, Schedule C forms as part of their PPP applications. Furthermore, no other business-related tax documents for these businesses had been filed with the IRS either. In total, I discovered that the likely fraudulent PPP loan applications associated with **CALHOUN** resulted in individuals being approved for $531,111.33 in PPP loans and having received $400,632.00.

15. Records were subpoenaed from Itria Ventures LLC, a financial institution that had received a Paycheck Protection Program (PPP) Borrower Application Form for the business "Partied by Jazz." This PPP application contained **CALHOUN**'s signature, personal address, social security number, and listed **CALHOUN** as the 100% owner of "Partied by Jazz". The application showed that the businesses payroll was $8,850 per month and that one employee worked at the business. The loan request amount on the application was $20,833, which was

cancelled before it could be disbursed. This application contained indicators of fraud that had also been identified on the other PPP applications, believed to be associated with **CALHOUN**. Furthermore, a picture of the front and back of **CALHOUN**'s Wisconsin Driver's License, a BMO Harris bank statement in **CALHOUN**'s name, and a blank IRS Schedule C were also submitted to Itria Venutures LLC as part of the PPP application package for "Partied by Jazz". IRS records show that **CALHOUN** had filed a 2020 Application for Employer Identification Number (Form SS-4)[1] with the IRS. On the Form SS-4, **CALHOUN** had listed herself as the sole proprietor for "Partied by Jazz." However, since that time, no other business records for "Partied by Jazz," such as an Employer's Annual Federal Unemployment Tax Return (Form 940)[2], or an Employer's Quarterly Federal Tax Return (Form 941)[3] have been filed with the IRS. **CALHOUN** also did not report any income from "Partied by Jazz" on her personal tax returns by filing a Form Schedule C (Sole Proprietorship Profit or Loss from Business) or report any wages from "Partied by Jazz" on her Form 1040.

Meta Subpoena and Warrant

16. On August 29, 2022, Meta Platforms, Inc. (Meta) records pertaining to **CALHOUN**'s Facebook accounts "Princess Jasmine" and "Partii PartiedbyJazz" were subpoenaed. Both Facebook accounts had posts, believed to have been made by **CALHOUN,**

---

[1] Form SS-4 is used to apply for an employer identification number (EIN). An EIN is a 9-digit number assigned to employers, sole proprietors, corporations, partnerships, estates, trusts, certain individuals, and other entities for tax filing and reporting purposes.

[2] Form 940 is used to report an employer's annual Federal Unemployment Tax Act (FUTA) tax. Together with state unemployment tax systems, the FUTA tax provides funds for paying unemployment compensation to workers who have lost their jobs.

[3] Form 941 is used to report income taxes, Social Security tax, or Medicare tax withheld from employee's paychecks. It is also used to pay the employer's portion of Social Security or Medicare tax.

advertising her tax preparation and PPP loan services. The records provided by Meta had shown that the "Princess Jasmine" account was registered with Facebook on September 15, 2009, and that the "Partii PartiedbyJazz" account was registered with Facebook on January 26, 2020. Furthermore, the phone number 414-719-3818, the AT&T phone number registered to **CALHOUN**, was listed when creating both Facebook accounts.

17. On December 6, 2022, United States Magistrate Judge William Duffin issued a search warrant to Meta for records and other information pertaining to the Facebook accounts, "Princess Jasmine" and "Partii PartiedbyJazz", to search for evidence of the crimes described in this affidavit. On December 6, 2022, Meta was served the aforementioned warrant. The records were produced by Meta on December 20, 2022. Within these records were numerous private Facebook messages between **CALHOUN** and different Facebook users. In many of these conversations, individuals would solicit **CALHOUN**'s services for tax preparation, assistance with PPP loan applications, and to obtain other fraudulent documents.

18. As I reviewed the Facebook records, I saw multiple conversations in which **CALHOUN** would request that individuals send tax documents to her electronically. **CALHOUN** would then provide clients different email addresses to send the documents to. Two of these email addresses contained the word "tax" or "tax service."

19. For example, on March 26th, 2022, a Facebook user with the username "Elle Porter" messaged **CALHOUN** asking about the status of her tax refund. "Elle Porter" was later identified through public records as being Lashunda McNeal (McNeal). McNeal followed-up her message by asking for **CALHOUN**'s email address, so that she could send **CALHOUN** a

transcript[4]. **CALHOUN** replied to McNeal's message by telling McNeal to send the transcript to **Freedomtaxxes@gmail.com (Target Account 1)**. McNeal then told **CALHOUN** that she had sent the transcript from the email address mcneallash@gmail.com.

20. On April 11th, 2022, **CALHOUN** messaged McNeal on Facebook Messenger, saying that she had sent McNeal an email. **CALHOUN** sent a screenshot of the email that she had sent to McNeal. The screenshot showed that the email was sent to mcnealash@gmail.com from the email address **maxxedfinancial@gmail.com (Target Account 3).** The email stated "Ms. McNeal, please see attached documents for 2021 tax return" along with a PDF attachment titled "2021_TaxReturn (83)".

21. On the "Princess Jasmine" Facebook account, I previously saw **CALHOUN** list herself as the owner of "Freedom's Tax Services." Furthermore, when reviewing **CALHOUN**'s Facebook Messages, I saw that **CALHOUN** would send new clients a list of documents needed to complete their tax returns. This list was titled "Freedom's Tax Services, New Client Checklist." IRS databases had previously been searched for any records or business filings for "Freedom's Tax Services." No employer identification number or business records for Freedom's Tax Services were located. **CALHOUN** also did not file any tax returns or report any income from this business on her own tax returns during tax years 2017-2021.

22. IRS databases were then used to review McNeal's 2021 Form 1040, which was filed from IP Address 76.196.89.6. AT&T records had previously shown this IP Address to be registered to **CALHOUN**. McNeal's 2021 Form 1040 showed that she had earned wages totaling

[4] It is believed that McNeal was likely referring to an IRS transcript, which would have summarized McNeal's previous tax filing history with the IRS.

$18,999 without any Form W-2 to support such wage earnings. Furthermore, this was the exact same wage amount found on 33 other tax returns associated with **CALHOUN**. McNeal's 2021 Form 1040 showed that she had claimed the Earned Income Credit and American Opportunity Credit. On the American Opportunity Credit, McNeal listed MATC as the institution she attended. There was no corresponding 1098-T filed by MATC to support McNeal's attendance. The indicators of fraud found on McNeal's 2021 Form 1040 were also found on the 273 other tax returns associated with **CALHOUN**.

23. On January 12th, 2021, a Facebook user with the username "LarQuita Henderson" sent **CALHOUN** a message, asking if **CALHOUN** needs her Form W-2. "Larquita Henderson" also told **CALHOUN** to work her magic. Public records were used to confirm Larquita Henderson's (Henderson) identity as being the same as her Facebook username. On February 4th, 2021, Henderson again messaged **CALHOUN**, stating that she now had her Form W-2 and asked when **CALHOUN** would be ready for her. **CALHOUN** responded to Henderson with the email address **Maxxedtaxservices@gmail.com (Target Account 2)**. Based on my training and experience, I believe that **CALHOUN** had sent this email address to Henderson, to receive all of the documents needed to prepare Henderson's 2020 Form 1040.

24. I then reviewed IRS records for Henderson's 2020 Form 1040, which was also filed from the same 76.196.89.6 IP Address belonging to **CALHOUN**. Henderson's 2020 Form 1040 showed reported wages of $19,354. However, Henderson's Form W-2 had shown that she had actually only earned wages totaling $11,354. Like the other tax returns associated with **CALHOUN**, Henderson's 2020 Form 1040 showed that she had claimed the American Opportunity Credit, Additional Child Tax Credit, and Earned Income Credit. In the American Opportunity Credit, Henderson had listed MATC as the institution that she attended, without any

corresponding 1098-T having been filed by MATC. By inflating Henderson's wages and claiming tax credits listed above, **CALHOUN** was able to get Henderson a much higher tax refund totaling $9,451.

Facebook Post

25. On January 11th, 2023, I utilized an undercover Facebook account to see if **CALHOUN** had made any recent Facebook posts about tax preparation on the "Princess Jasmine" account. I saw that a few minutes earlier, **CALHOUN** had posted "Now accepting new and returning clients. E-file today. See if you qualify for cash advances, MAX GUARENTEED." Below the post, was a flyer for "Freedom's Tax Services" that had a picture of **CALHOUN**. On the flyer was **CALHOUN**'s 414-719-3818 phone number and the email address **maxxedfinancial@gmail.com (Target Account 3)**. A screenshot of the post is below:

January 11, 2023, Facebook Post Advertising Tax Services

Google Subpoena

26. On January 25, 2023, I served Google with a subpoena to determine the individual who **Target Account 1**, **Target Account 2**, and **Target Account 3** are registered to. I received the requested records from Google on the same day. The records showed that **Target Account 1** was created on January 14, 2022. The "Recovery SMS" listed for **Target Account 1** is the phone number 414-719-3818, which per AT&T records is registered to **CALHOUN**. Furthermore, the IP Activity for **Target Account 1**, shows the IP Address used during several account logins to be 76.196.89.6, which per AT&T records is also registered to **CALHOUN**.

27. **Target Account 2** was created on December 24, 2020. The "recovery e-mail" listed for **Target Account 2** is speedydocuments75@gmail.com. When reviewing **CALHOUN**'s Facebook messages, I had seen **CALHOUN** tell clients to send items needed for the creation of fake documents such as bank statements, check stubs, housing packages, and doctor excuses to that e-mail address. The "recovery SMS" listed for **Target Account 2** is 262-409-7252, which per T-Mobile records, is registered to **CALHOUN**.

28. **Target Account 3** was created on March 5, 2021. The "recovery e-mail" listed for **Target Account 3** is also speedydocuments75@gmail.com, while the "recovery SMS" for **Target Account 3** is the same 414-719-3818, that is registered to **CALHOUN**. Furthermore, the IP Activity for **Target Account 3**, shows the same 76.196.89.6 IP Address, belonging to CALHOUN, used several times during different account login periods.

Background Concerning Email

29. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

30. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the internet must use an IP address, IP address information can help identify which computers or other devices were used to access the email account.

31. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

32. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, where, when, why, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the

information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

33. In general, an email that is received is stored in the subscriber's "mailbox" on a service provider's server until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on a server indefinitely. Even if the subscriber deletes the email, it may continue to be available on a server for a period of time.

34. On January 20, 2023, Google LLC was sent a Request for Preservation of Records Letter pursuant to Title 18 U.S.C. § 2703(f) via Google LLC's Law Enforcement Request System. This letter requested Google LLC preserve, among other things, all stored communications, records, and other evidence regarding accounts previously mentioned. Google LLC has assigned 29781545 as the reference number to this request.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

35. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google, LLC to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

36. Based on the forgoing, I request that the Court issue the proposed search warrant.

37. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving it on Google, LLC. Because the warrant will be served on Google, LLC who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the following Gmail accounts:

a. Gmail Account: **freedomtaxxes@gmail.com (Target Account 1)**

b. Gmail Account: **maxxedtaxservices@gmail.com (Target Account 2)**

c. Gmail Account: **maxxedfinancial@gmail.com (Target Account 3)**

which are stored at premises owned, maintained, controlled, or operated by Google, LLC, a company headquartered in Mountain View, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google, LLC (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to the Provider, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on January 20, 2023 (number 29781545), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A **for the time period of December 24, 2020, through the date of this warrant for all target accounts:**

(a) All records or other information regarding the identification of the accounts, commonly known as subscriber or registration information, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses, methods of connecting, log files, and means and source of payment (including any credit or bank account number).

(b) The types of services utilized.

(c) The contents of all emails associated with the accounts, including stored or preserved copies of emails sent to and from the accounts, draft emails, the source, and destination addresses associated with each email, the date and time at which

each email was sent, the size and length of each email, and any attachments associated with emails.

(d) The details of electronic devices used to access such services such as serial numbers and other unique device identification numbers.

(e) All other records or other information stored using the accounts, including address books, contact lists, calendar data, pictures and videos, and files.

(f) All records pertaining to communications between the provider and any person(s) regarding the accounts, including contacts with support services and records of actions taken.

The provider is hereby ordered to disclose the above information to the government **14 DAYS** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. 286 (Conspiracy to Defraud the Government), 18 U.S.C. 287 (Filing False Claims), 18 U.S.C. 1343 (Wire Fraud), and 26 U.S.C. 7206(2) (Aid or Assist in Filing False or Fraudulent Returns) involving **JASMINE CALHOUN** including, information pertaining to the following matters:

1. The creation, preparation, and filing of tax returns, including all preparatory steps and communications.
2. Information provided by clients and potential clients concerning potential tax returns and Paycheck Protection Program loans.

3. Records and information pertaining to taxes, refunds, and W-2s.
4. Advertisements and/or solicitation of tax clients.
5. Stimulus checks and Paycheck Protection Program Applications
6. Personal identifiable information of taxpayers, including names, date of birth, social security numbers, and driver's licenses.
7. Mailings to and from 3907 N. 84th St Milwaukee, WI 53222 including in names other than **JASMINE CALHOUN**.
8. Proceeds and/or payments pertaining to the preparation of tax returns or Paycheck Protection Program Applications.
9. Financial records, including account information, bank statements, checks, money orders, cash, ATMs, withdrawals, deposits, transfers (including wire, ACH transfers);
10. All evidence of who created, used, owned or controlled the Target Accounts, including, records that help reveal the identity and whereabouts of such person(s).
11. Evidence indicating how and when the Target Accounts were accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crimes under investigation and to the Target Account owner.
12. Evidence indicating the Target Account(s) owner's state of mind as it relates to the crimes under investigation.
13. The identity of the person(s) who communicated with the Target Accounts about matters relating to the above-mentioned violations, including records that help reveal their whereabouts.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google LLC ("Google"), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google. The attached records consist of _____ **[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]**. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, and they were made by Google as a regular practice; and

b. such records were generated by Google's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature